Solutions. Experts. Insights.

SEI TECHNOLOGIES FORUM

Software Engineering Institute | Carnegie Mellon

Software, Security, and Resiliency

Paul Nielsen
SEI Director and CEO

Dr. Paul D. Nielsen is the Director and CEO of Carnegie Mellon University's Software Engineering Institute. Under Dr. Nielsen's leadership, the SEI has expanded its research, doubled its staff and increased its impact in the software engineering community. The SEI now has over 500 valued partnerships with organizations extending its influence globally. Prior to joining SEI in 2004, he served in the U.S. Air Force, retiring as a major general and commander of Air Force research after 32 years of distinguished service. Nielsen is a member of the US National Academy of Engineering (NAE) and a Fellow of both the American Institute of Aeronautics and Astronautics (AIAA) and the Institute for Electrical and Electronics Engineers (IEEE).

© 2011 Carnegie Mellon University

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
FEB 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Software, Security, and Resiliency	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University ,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**15**	

Software and Complexity

© 2011 Carnegie Mellon University

The Rise of Complexity

- Scale
- Interconnectedness
- Autonomy
- Time criticality
- Security
- Safety
- Regulation

© 2011 Carnegie Mellon University

How to Handle Complexity

Models

Process

Architecture

Risk assessment

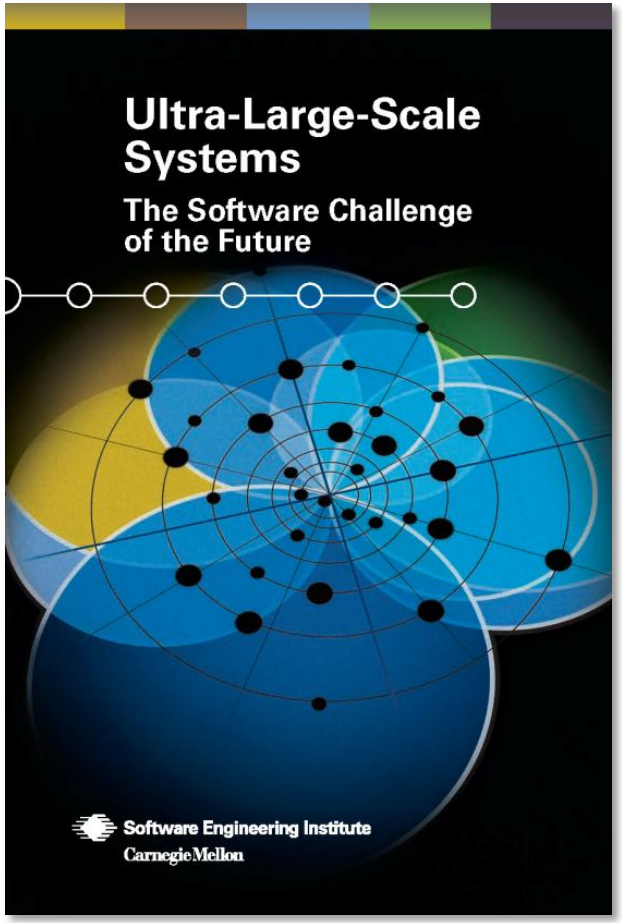
Resiliency

Evolution

People

© 2011 Carnegie Mellon University

Complex Systems at the SEI



The SEI is at the nexus of systems and complexity:

- We study them side-by-side
- For 25 years, we've been helping engineers design and manage software systems
- It's our job to "ring the bell" on the importance of managing complexity

We also appreciate risk and the importance of managing it

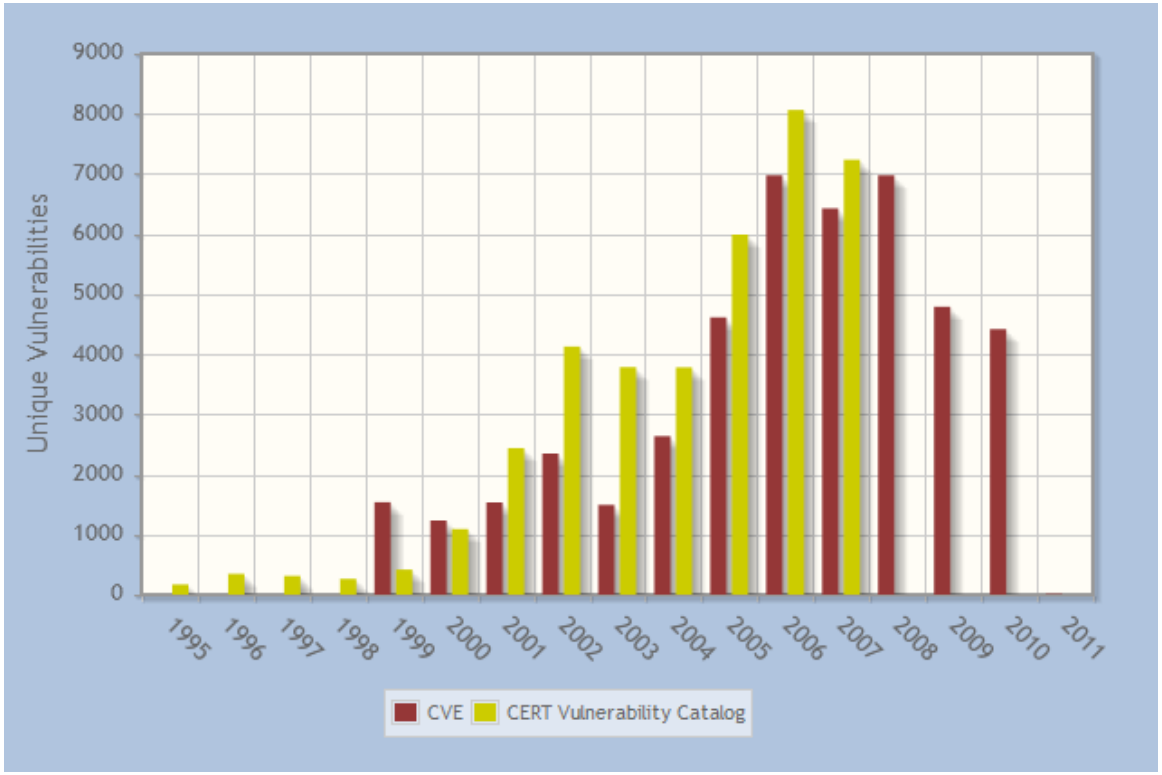
- Continuous risk management
- Mosaic suite of risk management tools
- Multi-view models
- Mission Success in Complex Environments

© 2011 Carnegie Mellon University

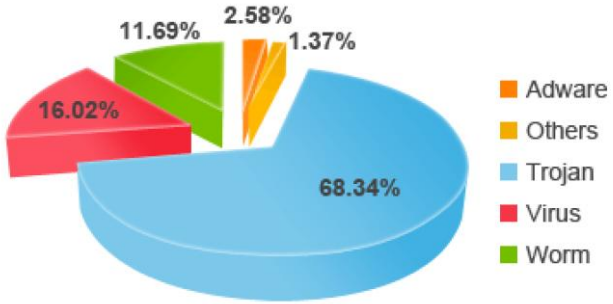
Security and Risk

© 2011 Carnegie Mellon University

Rising Tide of Vulnerabilities, Risk



Unique Vulnerabilities
(from CERT and NIST NVD data)



Recent Pandalabs Analysis of
Malware, Viruses in Circulation

© 2011 Carnegie Mellon University

How to Handle Cyber Security Issues

Secure Coding

Malware Identification and Analysis

Network Situational Awareness

Recognizing Insider Threats

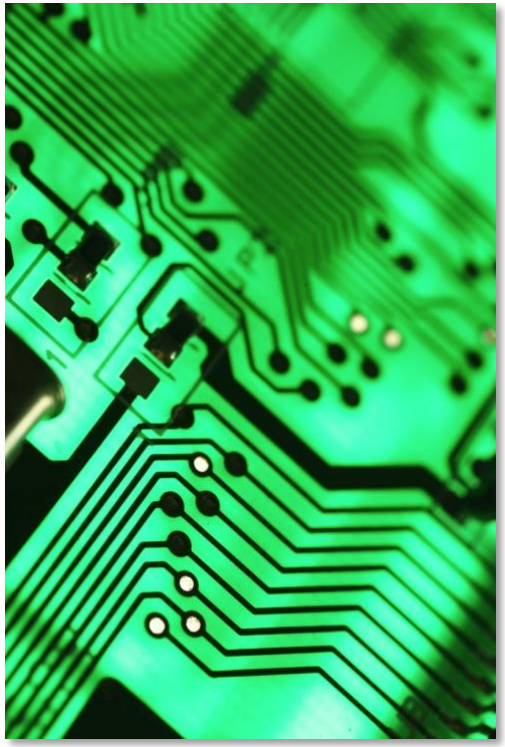
Modeling Resiliency and Continuity

© 2011 Carnegie Mellon University

Resiliency and Continuity

© 2011 Carnegie Mellon University

Key Principles of Resiliency (1)



Resilience is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.

At SEI, both organizational and software:

- Resilience Maturity Model (RMM)
- Security Quality Requirements Engineering (SQUARE)
- **security "built in"**
- Current blog series topic (http://blog.sei.cmu.edu/)
- **failure scenarios understood, planned for**
- **redundancy is provided for in key areas**
- **capability remains available under adverse conditions**

resilience

© 2011 Carnegie Mellon University

Continuity

A key aim of resiliency (and managing operational risk)

Business Functions:

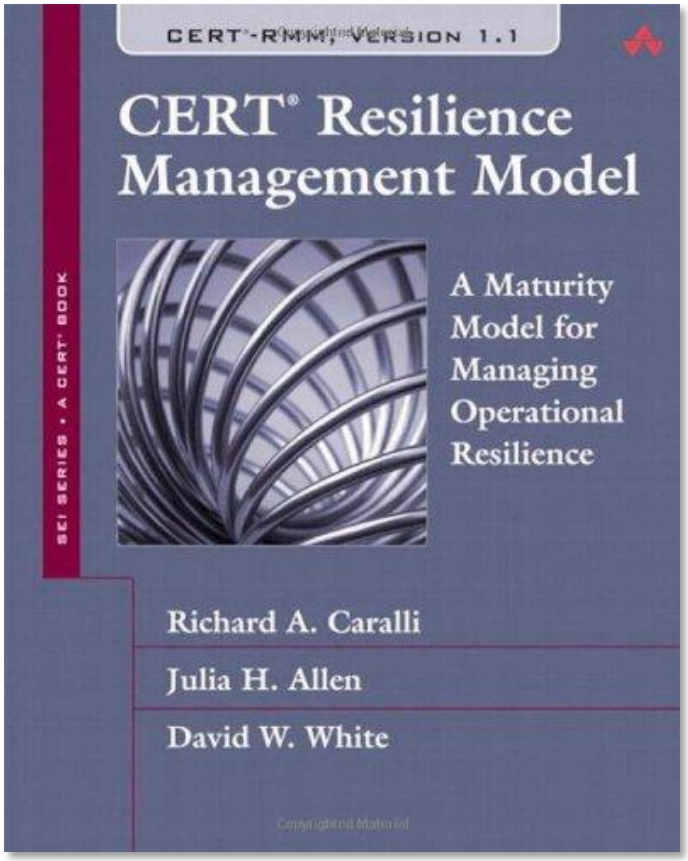
- Developing and executing continuity plans, recovery plans, and restoration plans

IT Function:

- Developing, implementing, and managing processes to deliver IT services and manage IT infrastructures

© 2011 Carnegie Mellon University

Resiliency Maturity Model (1)



What is CERT-RMM?

CERT-RMM is a maturity model for managing and improving operational resilience.

- Guides implementation and management of operational resilience activities
- Converges key operational risk management activities: security, business continuity/disaster recovery, and IT operations
- Defines maturity through capability levels (like CMMI)
- Improves confidence in how an organization responds in times of operational stress

© 2011 Carnegie Mellon University

Connecting the Dots

Today's presentations include:

Understanding and coping with complexity & cyber security

- CMMI-SVC: The Strategic Landscape for Service
- Software Acquisition Program Dynamics
- Architectural Implications of Cloud Computing
- The Insider Threat: Lessons Learned from Actual Insider Attacks

Dealing with the smart grid, resiliency and software development

- Smart Grid Maturity Model
- Agile Development and Architecture: Understanding Scale and Risk
- Measuring Operational Resilience
- Team Software Process (TSP)

© 2011 Carnegie Mellon University

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

© 2011 Carnegie Mellon University

Contact Information

Paul Nielsen
Director and CEO
Software Engineering Institute
Telephone: +1 412-268-7740
Email: nielsen@sei.cmu.edu

U.S. Mail
Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

Web
www.sei.cmu.edu
www.sei.cmu.edu/contact.cfm

Customer Relations
Email: info@sei.cmu.edu
Telephone: +1 412-268-5800
SEI Phone: +1 412-268-5800
SEI Fax: +1 412-268-6257

© 2011 Carnegie Mellon University